

expense balanced against the degree of sensitivity of the type of FOUO information contained in the records.

(2) Record copies of FOUO documents shall be disposed of in accordance with the disposal standards established under 44 U.S.C. chapter 33, as implemented by Inspector General Defense Manual (IGDM) 5015.2,⁴ "Records Management Program".

C. Unauthorized Disclosure

The unauthorized disclosure of FOUO records does not constitute an unauthorized disclosure of DoD information classified for security purposes. Appropriate administrative action shall be taken, however, to fix responsibility for unauthorized disclosure whenever feasible, and appropriate disciplinary action shall be taken against those responsible. Unauthorized disclosure of FOUO information that is protected by the Privacy Act may also result in civil and criminal sanctions against responsible persons. The DoD Component that originated the FOUO information shall be informed of its unauthorized disclosure.

APPENDIX B TO PART 295—EXEMPTIONS

I. General

The exemptions listed apply to categories of records that may be withheld in whole or in part from public disclosure, unless otherwise prescribed by law. A discretionary release (see also §295.5(e) of this part) to one requester may preclude the withholding of the same record under a FOIA exemption if the record is subsequently requested by someone else. In applying the exemptions, the identity of the requester and the purpose for which the record is sought are irrelevant with the exception that an exemption may not be invoked where the particular interest to be protected is the requester's interest. The examples provided of the types of records that may be exempted from release are not at all inclusive.

II. FOIA Exemptions

A. Exemption (b)(1).

Those properly and currently classified in the interest of national defense or foreign policy, as specifically authorized under the criteria established by executive order and implemented by regulations, such as DoD 5200.1-R¹ (32 CFR part 159a), "Information

Security Program Regulation". Although material is not classified at the time of the FOIA request, a classification review may be undertaken to determine whether the information should be classified. The procedures in DoD 5200.1-R, section 2-204f, apply. In addition, this exemption shall be invoked when the following situations are apparent:

(1) The fact of the existence or nonexistence of a record would itself reveal classified information. In this situation, the OIG shall neither confirm nor deny the existence or nonexistence of the record being requested. A "refusal to confirm or deny" response will be used consistently, not only when a record exists, but also when a record does not exist. Otherwise, the pattern of using a "no record" response when a record does not exist will itself disclose national security information.

(2) Information that concerns one or more of the classification categories established by executive order and DoD 5200.1-R (32 CFR part 159a) shall be classified if its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security.

B. Exemption (b)(2)

Those related solely to the internal personnel rules and practices of DoD or the OIG. This exemption has two profiles, *high (b)(2)* and *low (b)(2)*.

(1) Records qualifying under high (b)(2) are those containing or constituting statutes, rules, regulations, orders, manuals, directives, and instructions the release of which would allow circumvention of these records, thereby substantially hindering the effective performance of a significant function of the DoD or OIG. Examples include:

(a) Those operating rules, guidelines, and manuals, for DoD and OIG investigators, inspectors, auditors, or examiners that must remain privileged in order for the OIG to fulfill a legal requirement.

(b) Personnel and other administrative matters, such as examination questions and answers used in training courses or in the determination of the qualification of candidates for employment, entrance on duty, advancement, or promotion.

(c) Computer software meeting the standards of §295.3(c) of this part, the release of which would allow circumvention of a statute or DoD rules, regulations, orders, manuals, directives, or instructions. In this situation, the use of the software must be closely examined to ensure a circumvention possibility exists.

(2) Records qualifying under the low (b)(2) profile are those that are trivial and house-keeping in nature for which there is no legitimate public interest or benefit to be gained by release, and it would constitute an administrative burden to process the request

⁴Copies may be obtained, if needed, from the Information and Operations Support Directorate, Publications Management Branch, room 420, 400 Army Navy Drive, Arlington, VA 22202-2884.

¹Copies may be obtained, at cost, from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.

in order to disclose the records. Examples include: rules of personnel's use of parking facilities or regulation of lunch hours, statements of policy as to sick leave, and trivial administrative data such as file numbers, mail routing stamps, initials, data processing notations, brief references to previous communications, and other like administrative markings.

C. Exemption (b)(3)

Those concerning matters that a statute specifically exempts from disclosure by terms that permit no discretion on the issue, or in accordance with criteria established by that statute for withholding or referring to particular types of matters to be withheld. Examples of statutes are:

- (1) National Security Agency Act information exemption, Public Law 86-36, section 6.
- (2) Patent Secrecy, 35 U.S.C. 181-188. Any records containing information relating to inventions that are the subject of patent applications on which Patent Secrecy Orders have been issued.
- (3) Restricted Data and Formerly Restricted Data, 42 U.S.C. 2162.
- (4) Communication intelligence, 18 U.S.C. 798.
- (5) Authority to Withhold from Public Disclosure Certain Technical Data, 10 U.S.C. 130, and 32 CFR part 250.
- (6) Confidentiality of Medical Quality Records: Qualified Immunity Participants, 10 U.S.C. 1102.
- (7) Physical Protection of Special Nuclear Material: Limitation on Dissemination of Unclassified Information, 10 U.S.C. 128.
- (8) Protection of Intelligence Sources and Methods, 50 U.S.C. 403(d)(3).

D. Exemption (b)(4)

Those containing trade secrets or commercial or financial information that the OIG receives from a person or organization outside the Government with the understanding that the information or record will be retained on a privileged or confidential basis in accordance with the customary handling of such records. Records within the exemption must contain trade secrets, or commercial or financial records, the disclosure of which is likely to cause substantial harm to the competitive position of the source providing the information; impair the Government's ability to obtain necessary information in the future; or impair some other legitimate Government interest. Examples include:

- (1) Commercial or financial information received in confidence in connection with loans, bids, contracts, or proposals, as well as other information received in confidence or privileged, such as trade secrets, inventions, discoveries, or other proprietary data. See also 32 CFR part 286h, "Release of Acquisition-Related Information".

- (2) Statistical data and commercial or financial information concerning contract performance, income, profits, losses, and expenditures, if offered and received in confidence from a contractor or potential contractor.

- (3) Personal statements given in the course of inspections, investigations, or audits, when such statements are received in confidence from the individual and retained in confidence because they reveal trade secrets or commercial or financial information normally considered confidential or privileged.

- (4) Financial data provided in confidence by private employers in connection with locality wage surveys that are used to fix and adjust pay schedules applicable to the prevailing wage rate of employees within the Department of Defense.

- (5) Scientific and manufacturing processes or developments concerning technical or scientific data or other information submitted with an application for a research grant, or with a report while research is in progress.

- (6) Technical or scientific data developed by a contractor or subcontractor exclusively at private expense, and technical or scientific data developed in part with Federal funds and in part at private expense, wherein the contractor or subcontractor has retained legitimate proprietary interest in such data in accordance with title 10, U.S.C. 2320-2321 and DoD Federal Acquisition Regulation Supplement (DFARS), subpart 27.4 (see section C.(5) of this appendix).

- (7) Computer software meeting the conditions of §295.3(c), which is copyrighted under the Copyright Act of 1976 (17 U.S.C. 106), the disclosure of which would have an adverse impact on the potential market value of a copyrighted work.

E. Exemption (b)(5)

Except as provided in subsections (2) through (5), below, internal advice, recommendations, and subjective evaluations, as contrasted with factual matters, that are reflected in records pertaining to the decision-making process of an agency, whether within or among agencies (as defined in 5 U.S.C. 552(e)), DoD Components or OIG components. Also exempted are records pertaining to attorney-client privilege and the attorney work-product privilege.

- (1) Examples include:

- (a) The nonfactual portions of staff papers, to include after-action reports and situation reports containing staff evaluations, advice, opinions, or suggestions.

- (b) Advice, suggestions, or evaluations prepared on behalf of the Department of Defense by individual consultants or by boards, committees, councils, groups, panels, conferences, commissions, task forces, or other similar groups that are formed for the purpose of obtaining advice and recommendations.

(c) Those non-factual portions or evaluations by DoD or OIG Components personnel of contractors and their products.

(d) Information of a speculative, tentative, or evaluative nature of such matters as proposed plans to procure, lease or otherwise acquire and dispose of materials, real estate, facilities or functions, when such information would provide undue or unfair competitive advantage to private personal interests or would impede legitimate Government functions.

(e) Trade secret or other confidential research development, or commercial information owned by the Government, where premature release is likely to affect the Government's negotiating position or other commercial interests.

(f) Records that are exchanged among agency personnel and within and among DoD Components or agencies as part of the preparation for anticipated administrative proceeding by an agency or litigation before any Federal, state, or military court, as well as records that qualify for the attorney-client privilege.

(g) Those portions of official reports of inspection, reports of the Inspector General, audits, investigations, or surveys pertaining to safety, security, or the internal management, administration, or operation of one or more DoD Components, when these records have traditionally been treated by the courts as privileged against disclosure in litigation.

(h) Computer software meeting the standards of §295.3(c), which is deliberative in nature, the disclosure of which would inhibit or chill the decision-making process. In this situation, the use of software must be closely examined to ensure its deliberative nature.

(i) Planning, programming, and budgetary information which is involved in the defense planning and resource allocation process.

(2) If any such intra or interagency record or reasonably segregable portion of such record hypothetically would be made available routinely through the "discovery process" in the course of litigation with the agency, i.e., the process by which litigants obtain information from each other that is relevant to the issues in a trial or hearing, then it should not be withheld from the general public even though discovery has not been sought in actual litigation. If, however, the information hypothetically would only be made available through the discovery process by special order of the court based on the particular needs of a litigant, balanced against the interests of the agency in maintaining its confidentiality, then the record or document need not be made available under this part. Consult with legal counsel to determine whether exemption 5 material would be routinely made available through the discovery process.

(3) Intra or interagency memoranda or letters that are factual, or those reasonably segregable portions that are factual, are routinely made available through "discovery," and shall be made available to a requester, unless the factual material is otherwise exempt from release, inextricably intertwined with the exempt information, so fragmented as to be uninformative, or so redundant of information already available to the requester as to provide no new substantive information.

(4) A direction or order from a superior to a subordinate, though contained in an internal communication, generally cannot be withheld from a requester if it constitutes policy guidance or a decision, as distinguished from a discussion of preliminary matters or a request for information or advice that would compromise the decision-making process.

(5) An internal communication concerning a decision that subsequently has been made a matter of public record must be made available to a requester when the rationale for the decision is expressly adopted or incorporated by reference in the record containing the decision.

F. Exemption (b)(6)

Information in personnel and medical files, as well as similar personal information in other files, that, if disclosed to the requester would result in a clearly unwarranted invasion of personal privacy. Release of information about an individual contained in a Privacy Act System of records would constitute a clearly unwarranted invasion of privacy is prohibited, and could subject the releaser to civil and criminal penalties.

(1) Examples of other files containing personal information similar to that contained in personnel and medical files include:

(a) Those compiled to evaluate or adjudicate the suitability of candidates for civilian employment or membership in the Armed Forces, and the eligibility of individuals (civilian, military, or contractor employees) for security clearances, or for access to particularly sensitive classified information.

(b) Files containing reports, records, and other material pertaining to personnel matters in which administrative action, including disciplinary action, may be taken.

(2) Home addresses are normally not releasable without the consent of the individuals concerned. In addition, the release of lists of DoD military and civilian personnel's names and duty addresses who are assigned to units that are sensitive, routinely deployable, or stationed in foreign territories can constitute a clearly unwarranted invasion of personal privacy.

(a) Privacy interest. A privacy interest may exist in personal information even though the information has been disclosed at

some place and time. If personal information is not freely available from sources other than the Federal Government, a privacy interest exists in its nondisclosure. The fact that the Federal Government expended funds to prepare, index and maintain records on personal information, and the fact that a requester invokes FOIA to obtain these records indicates the information is not freely available.

(b) Published telephone directories, organizational charts, rosters and similar materials for personnel assigned to units that are sensitive, routinely deployable, or stationed in foreign territories are withholdable under this exemption.

(3) This exemption shall not be used in an attempt to protect the privacy of a deceased person, but it may be used to protect the privacy of the deceased person's family.

(4) Individuals' personnel, medical, or similar file may be withheld from them or their designated legal representative only to the extent consistent with DoD Directive 5400.11 (32 CFR part 286a).

(5) A clearly unwarranted invasion of the privacy of the persons identified in a personnel, medical or similar record may constitute a basis for deleting those reasonably segregable portions of that record, even when providing it to the subject of the record. When withholding personal information from the subject of the record, legal counsel should first be consulted.

G. Exemption (b)(7)

Records or information compiled for law enforcement purposes; i.e., civil, criminal, or military law, including the implementation of executive orders or regulations issued pursuant to law. This exemption may be invoked to prevent disclosure of documents not originally created for, but later gathered for law enforcement purposes.

(1) This exemption applies, however, only to the extent that production of such law enforcement records or information could result in the following:

(a) Could reasonably be expected to interfere with enforcement proceedings.

(b) Would deprive a person of the right to a fair trial or to an impartial adjudication.

(c) Could reasonably be expected to constitute an unwarranted invasion of personal privacy of a living person, including surviving family members of an individual identified in such a record.

(i) This exemption also applies when the fact of the existence or nonexistence of a responsive record would itself reveal personally private information and the public interest in disclosure is not sufficient to outweigh the privacy interest. In this situation, the OIG shall neither confirm nor deny the existence or nonexistence of the record being requested.

(ii) A "refusal to confirm or deny" response must be used consistently, not only when a record exists, but also when a record does not exist. Otherwise, the pattern of using a "no records" response when a record does not exist and a "refusal to confirm or deny" when a record does exist will itself disclose personally private information.

(iii) Refusal to confirm or deny should not be used when (1) the person whose personal privacy is in jeopardy has provided the requester with a waiver of his or her privacy rights; or (2) the person whose personal privacy is in jeopardy is deceased, and the OIG is aware of that fact.

(d) Could reasonably be expected to disclose the identity of a confidential source, including a source within the Department of Defense, a State, local, or foreign agency or authority, or any private institution which furnishes the information on a confidential basis.

(e) Could disclose information furnished from a confidential source and obtained by a criminal law enforcement authority in a criminal investigation or by an agency conducting a lawful national security intelligence investigation.

(f) Would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

(g) Could reasonably be expected to endanger the life or physical safety of any individual.

(2) Examples include:

(a) Statements of witnesses and other material developed during the course of the investigation and all materials prepared in connection with related government litigation or adjudicative proceedings.

(b) The identity of firms or individuals being investigated for alleged irregularities involving contracting with Department of Defense when no indictment has been obtained nor any civil action filed against them by the United States.

(c) Information obtained in confidence, expressed or implied, in the course of a criminal investigation by a criminal law enforcement agency or office within a DoD Component, or a lawful national security intelligence investigation conducted by an authorized agency or office within a DoD Component. National security intelligence investigations include background security investigations and those investigations conducted for the purpose of obtaining affirmative or counterintelligence information.

(3) The right of individual litigants to investigative records currently available by law (such as, the Jencks Act, 18 U.S.C. 3500) is not diminished.

(4) When the subject of an investigative record is the requester of the record, it may

Office of the Secretary of Defense

§ 296.4

be withheld only as authorized by DoD Directive 5400.11 (32 CFR part 286a).

(5) Exclusions. Excluded from the above exemptions are the following two situations as applicable to the Department of Defense and the OIG:

(a) Whenever a request is made which involves access to records or information compiled for law enforcement purposes, and the investigation or proceeding involves possible violation of criminal law where there is reason to believe that the subject of the investigation or proceeding is unaware of its pendency, and the disclosure of the existence of the records could reasonably be expected to interfere with enforcement proceedings, the OIG may, during only such times as that circumstance continues, treat the records or information as not subject to the FOIA. In such situation, the response to the requesters will state that no records were found.

(b) Whenever informant records maintained by a criminal law enforcement organization within the OIG under the informant's name or personal identifier are requested by a third party using the informant's name or personal identifier, the OIG may treat the records as not subject to the FOIA, unless the informant's status as an informant has been officially confirmed. If it is determined that the records are subject to exemption (b)(7), the response to the requester will state that no records were found.

H. Exemption (b)(8)

Those contained in or related to examination, operation or condition reports prepared by, on behalf of, or for the use of any agency responsible for the regulation or supervision of financial institutions.

I. Exemption (b)(9)

Those containing geological and geophysical information and data (including maps) concerning wells.

PART 296—NATIONAL RECONNAISSANCE OFFICE FREEDOM OF INFORMATION ACT PROGRAM REGULATION

Sec.

296.1 Purpose.

296.2 Definitions.

296.3 Indexes.

296.4 Procedures for request of records.

296.5 Appeals.

296.6 Reading room.

AUTHORITY: 5 U.S.C. 552, as amended.

SOURCE: 64 FR 71298, Dec. 21, 1999, unless otherwise noted.

§ 296.1 Purpose.

The purpose of this part is to provide policies and procedures for the National Reconnaissance Office (NRO) implementation of the Freedom of Information Act (5 U.S.C. 552 as amended) (FOIA), and to promote uniformity in the NRO FOIA program.

§ 296.2 Definitions.

The terms used in this part, with the exception of the following, are defined in 32 CFR part 286:

(a) *Freedom of Information Act appellate authority*. The Chief of Staff, NRO.

(b) *Initial denial authority*. The Chief, Information Access & Release Center NRO.

§ 296.3 Indexes.

(a) The NRO does not originate final orders, opinions, statements of policy, interpretations, staff manuals or instructions that affect a member of the public of the type covered by the indexing requirement of 5 U.S.C. 552(a)(2). The Director, NRO, has therefore determined, pursuant to pertinent statutory and executive order requirements, that it is unnecessary and impracticable to publish an index of the type required by 5 U.S.C. 552(a)(2), except the index noted in paragraph (b) of this section.

(b) A general index of FOIA-processed (a)(2) records shall be made available to the public, both in hard copy and electronically by December 31, 1999.

§ 296.4 Procedures for request of records.

(a) *Requests*. Requests for access to records of the National Reconnaissance Office may be filed by mail or FAX addressed to the Chief, Information Access and Release Center, National Reconnaissance Office, 14675 Lee Road, Chantilly, VA 20151-1715, FAX Number (703) 808-5082. Requests need not be made on any special form but must be by letter or FAX or other written statement identifying the request as a Freedom of Information Act request and setting forth sufficient information reasonably describing the requested record. All requests should contain a willingness to pay assessable FOIA fees.